UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/877,655	06/08/2001	Hovav Shacham	36321.8007.US	9498

22918 7590 10/20/2004

PERKINS COIE LLP
P.O. BOX 2168
MENLO PARK, CA 94026

EXAMINER	
SIMITOSKI, MICHAEL J	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 10/20/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/877,655	SHACHAM ET AL.	
	Examiner	Art Unit	
	Michael J Simitoski	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 June 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-32* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-32* is/are rejected.

7)☒ Claim(s) *6,13 and 18* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *18 October 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-32 are pending.

Specification

2. The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required: Hensle lifting is not described in the specification.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

4. Claims 1, 24-26 & 31-32 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention.

5. Regarding claim 1, if *p-1* and *q-1* are primes, then r_1 and r_2, by $d = r_1 \bmod(p-1)$ and $d = r_2 \bmod(q-1)$, would have to be equal for most numbers, as they are much smaller than p and q, which are typically 512 bits. As best understood, r_1 cannot be equal to r_2 in most situations, as this limitation would suggest.

6. Regarding claims 24-26 & 31-32, Hensle lifting is not described in the specification so as to enable this limitation in the claims. Hensle lifting, as best understood, if a mathematical method of modular exponentiation, and will be treated generically as such.

7. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

8. Claims 1-32 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Regarding claims 1-32, the various uses of the term "RSA" public or private keys or public/private key pairs render the claims indefinite, as RSA is a trademark. The scope of a RSA public/private key/key pair is determined by RSA and is therefore undetermined. Further, suggestions toward bit length (for instance, a 1024-bit modulus) change as cryptanalysis technology improves and therefore must be further defined.

Regarding claims 1, 5 & 16, the limitation "on the order of 160" is indefinite. *For the purposes of this Office Action, this is understood to mean the same order of magnitude.* Claims 2-4 & 6-8 are rejected based on their dependence on claims 1, 5 or 16.

Regarding claims 5, 9, 15, 17, 25, 29 & 30, the term "random" is understood to mean "randomly generated" (as is common in the art of cryptography), however, the random numbers ($< r_1, r_2 >$) in the application must satisfy the conditions, $d = r_1 \bmod(p-1)$ and $d = r_2 \bmod(q-1)$, and therefore it is unclear how the numbers are random. *For the purposes of this Office Action, the "random" numbers are assumed to be mathematically related to randomly generated numbers.*

Regarding claim 8, R_1' and R_2' do not appear in the equations claimed.

Regarding claim 9, line 8 recites "the RSA key" but it is unclear which key this refers to.

Regarding claims 9, 15, 29 & 30, the limitation "separating cipher-text moduli of the two distinct prime numbers; decrypting the moduli of the two distinct prime numbers ..." is indefinite; it is unclear whether the "[cipher-text] moduli of the two distinct prime numbers" represents the RSA modulus (N), the two prime numbers (p,q) or the result of taking the modulus using the two prime numbers, as the two random numbers appear to decrypt the cipher-text. *For the purposes of this Office Action, the "[cipher-text] moduli" refers to a number mod p, q or some mathematical manipulation of p or q.*

Regarding claims 9, 13, 17 & 25-32 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The term "efficiency" is indefinite. Claims 10-12, 14 & 18-20 are rejected based on their dependence on claims 9, 13, 17 & 25-32.

Regarding claim 14, the claim recites the limitation "size of N" in lines 1 & 4. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. Claims 1-5, 8 & 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Network Security Essentials: Applications and Standards by Stallings in view of Handbook of Applied Cryptography by Menezes et al. (Menezes) in view of "Homework 4 with Extensive Hints" by Immerman, in further view of "Cryptanalysis of Short RSA Secret Exponents" by Wiener.

Regarding claim 1, 2, 5, 8 & 15, Stallings discloses sending a client hello message to the web server from a client requesting a secure network connection/SSL, responding to the client with a server hello message comprising the RSA public key/certificate (page 214, Fig. 7.6 & ¶2), encrypting a random string R/pre-master secret at the client using the RSA public key, wherein the resulting cipher-text C includes R/pre-master secret (page 217, ¶4), sending the encrypted cipher-text to the web server/server, decrypting the cipher-text at the web server using the RSA private key (page 218, ¶5) and establishing a common session key between the web server and client using R/pre-master secret (page 218, ¶7). Stallings lacks generating a Rivest-Shamir-Adleman algorithm public/private key pair at a web server, wherein $< N, e' >$ represents the public key with N being the product of two distinct primes, p and q, and wherein the private key is represented by d, the RSA private key being such that $d = r_1 \bmod(p-1)$ and $d = r_2 \bmod(q-1)$ and wherein $< r_1, r_2 >$ are relatively small numbers on the order of 160 bits in length, wherein R'_1 equals the cipher-text raised to the r_1 power moduli one of the distinct prime numbers and R'_2 equals the cipher-text raised to the r_2 power moduli the remaining prime number and lacks combining R'_1 and R'_2 to produce R using the Chinese remainder Theorem wherein finding R'_1 and R'_2 is more efficient than using standard RSA keys. However, Menezes teaches standard RSA parameter generation, wherein (n,e) is the public key with n=pq (§8.2.1). Therefore, it

would have been obvious to one having ordinary skill in the art at the time the invention was made to generate a Rivest-Shamir-Adleman algorithm public/private key pair at a web server, wherein $< N, e' >$ represents the public key with N being the product of two distinct primes, p and q, and wherein the private key is represented by d. One of ordinary skill in the art would have been motivated to perform such a modification to use the RSA public key encryption/decryption function, as taught by Menezes (§8.2.1). Menezes further teaches that $x^d \bmod n$ (decryption) can be more efficiently computed using the pair $x^{d_p} \bmod p$ and $x^{d_q} \bmod q$ (equivalent to the claimed $C^{r_1} \bmod p$ and $C^{r_2} \bmod q$) and recombine the solution using the CRT/Garner's algorithm (§14.5.2, 14.75 Note). Further, Immerman teaches that using the Chinese Remainder Theorem, integers mod ab ($z = \text{int}(\bmod ab)$) can be written in terms of integers mod a ($x = \text{int}(\bmod a)$) and mod b ($y = \text{int}(\bmod b)$), such that $z \equiv x(\bmod a)$ and $z \equiv y(\bmod b)$ (page 1, §Chinese Remainder Theorem). Therefore, by the Chinese Remainder Theorem, $d_p = d(\bmod p-1)$ and $d_q = d(\bmod q-1)$ share the relationship $d = d_p(\bmod p-1)$ and $d = d_q(\bmod q-1)$, the decryption pair being $< d_p, d_q >$. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to have the RSA private key being such that $d = r_1 \bmod(p-1)$ and $d = r_2 \bmod(q-1)$, wherein R'_1 equals the cipher-text raised to the r_1 power moduli one of the distinct prime numbers and R'_2 equals the cipher-text raised to the r_2 power moduli the remaining prime number and combine R'_1 and R'_2 to produce R using the Chinese remainder Theorem. One of ordinary skill in the art would have been motivated to perform such a modification to more efficiently compute RSA decryption, as taught by Menezes (§14.5.2, 14.75 Note) and Immerman (page 1). Wiener

teaches that the shorter the exponents in RSA, the fast the decryption time (page 2, ¶2). Wiener also teaches exponents being up to ¼ the number of bits in the modulus (ABSTRACT), which is often 1024 (page 10, last ¶). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use a 256-bit exponent, which is on the order of 160 bits. One of ordinary skill in the art would have been motivated to perform such a modification to reduce encryption time, as taught by Wiener (page 2, ¶2).

Regarding claims 3-4, Stallings discloses TLS (page 219) and IPSec (page 163).

11. Claims 9-12 & 29-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stallings in view of "Twenty Years of Attacks on the RSA Cryptosystem" by Boneh.

Regarding claims 9-10 & 29-30, Stallings discloses coupling a client to a server (page 214, Fig. 7.6), sending a client hello message to the web server from a client requesting a secure network connection/SSL, responding to the client with a server hello message comprising the RSA public key/certificate (page 214, Fig. 7.6 & ¶2), encrypting a random string R/pre-master secret at the client using the RSA public key, wherein the resulting cipher-text C includes R/pre-master secret (page 217, ¶4), sending the encrypted cipher-text to the web server/server, decrypting the cipher-text at the web server using the RSA private key (page 218, ¶5) and establishing a common session key between the web server and client using R/pre-master secret (page 218, ¶7). Stallings lacks generating a Rivest-Shamir-Adleman (RSA) algorithm public/private key pair at the web server, wherein the RSA public key is a product of two distinct prime numbers and the private key is a function of two random numbers, wherein each random number has a number of bits greater than or equal to 160 bits and less than a number of bits of the RSA private key, separating the ciphter-text moduli of the two distinct prime numbers and

decrypting the moduli of the two distinct prime numbers individually using the two random numbers, wherein the results are combined using the Chinese Remainder Theorem. However, Boneh teaches generating a Rivest-Shamir-Adleman ("RSA") algorithm public/private key pair, the public key being the product of two distinct n-bit prime numbers, p and q, (page 203) where the private key is a function of two random numbers/ d_p and d_q, separating the cipher-text moduli of the two distinct prime numbers (p and q) individually using the two random numbers and decrypting the moduli of the two distinct prime numbers individually using the two random numbers, wherein the result are combined using the Chinese Remainder Theorem, wherein computational efficiency is improved (page 206). While Boneh gives an example of the two numbers being 128 bits, he makes the observation that *d* (the private key) should be greater than 1/3 of the size of the modulus *N*, possibly even greater than ½ (1024/3=~341 -- 1024/2=512 bits). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to generate the RSA pair, wherein the secret key is a function of two random numbers greater than 160 bits, separate the cipher-text moduli of the two distinct prime numbers, decrypt the moduli of the two distinct prime numbers individually and combine the results with the Chinese remainder theorem. One of ordinary skill in the art would have been motivated to perform such a modification to increase decryption speed, as taught by Boneh (pages 203-206).

Regarding claims 11-12, Stallings discloses TLS (page 219) and IPSec (page 163).

12. Claim 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over Stallings in view of Boneh, as applied to claim 9 above, in further view of U.S. Patent 5,848,159 to Collins et al. (Collins). Stallings, as modified above, lacks reducing the size of the two distinct prime numbers such that each of the two distinct prime numbers is on the order of one third the size of *N*.

However, Collins teaches that using multi-prime RSA, computational speed is increased (col. 3, lines 35-46). Using, for example 3 primes, each is 100 digits long, rather than a single one at 300 digits long (col. 3, lines 49-55). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to reduce the size of the two distinct prime numbers such that each of the two distinct prime numbers is on the order of one third the size of *N*. One of ordinary skill in the art would have been motivated to perform such a modification to make use of multi-prime RSA to increase computational speed, as taught by Collins (col. 3, lines 35-55).

13. Claim 16 is rejected under 35 U.S.C. 103(a) as being unpatentable over Boneh in view of Stallings. Boneh discloses generating a Rivest-Shamir-Adleman ("RSA") algorithm public/private key pair, the public key comprising a root *N*, wherein *N* of the RSA public key is the product of two distinct n-bit prime numbers, p and q, wherein an encryption component e' of the RSA public key is of the same order in size (about 700 bits) as the public key root *N* (1024 bits) (page 206) and encrypting a plain-text message R/*M* using the RSA public key such that the resulting text is cipher-text C (page 203), decrypting the cipher-text C using the RSA private key wherein the RSA private key is a function of two roots r_1/d_p and r_2/d_q wherein the two roots each are on the order of 160 bits in length (about 256 bits) (page 206). Boneh lacks using the plain-text message R to determine a session encryption key and a session integrity key. However, Stallings teaches that the SSL protocol, which commonly uses RSA (page 214), to encrypt/decrypt a pre-master secret (page 217) to generate a session key/master secret and an integrity key/MAC secret (page 218). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to determine a session encryption key

and a session integrity key using the plain-text message R. One of ordinary skill in the art would have been motivated to perform such a modification to use Boneh's encryption scheme in the SSL protocol, as taught by Stallings (pages 214, 217 & 218).

14. Claims 17 & 27-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stallings in view of Menezes, Immerman & Wiener, in further view of "Fast RSA-type cryptosystem modulo $p^k q$" by Takagi.

Regarding claim 17, the claim is substantially equivalent to claim 1 and is rejected under similar rationale, except Stallings, as modified, lacks keeping the size of N constant while reducing the size of the two distinct prime numbers by calculating N from a product of a first distinct prime number raised to the first power and a second distinct prime number wherein the first power is greater than one and constructing an additional $R"_1$ using one of the two distinct prime numbers raised to a power greater than one, wherein efficiency of the decryption is increased. However, Takagi teaches that by performing $n = p^k q$, the system is protected from both the number field sieve and elliptic curve methods of attack (§1 & §3 ¶2-3) where p and q are over 256 bits and n is over 768 bits (rather than $n=pq$, where if n is 768 bits, then p and q would be 384 bits). This system is faster than standard RSA (§4, last ¶). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to reduce the size of the two distinct prime numbers while keeping the size of the public key root constant using exponentiation of the two distinct prime numbers and construct an additional $R"_1$ using one of the two distinct prime numbers raised to a power greater than one/k. One of ordinary skill in the art would have been motivated to perform such a modification to protect the system from attack and to increase speed, as taught by Takagi (§1, §3 ¶2-3 & §4 last ¶).

Regarding claims 27-28, the claims are substantially equivalent to claim 1 and are rejected under similar rationale, except Stallings, as modified, lacks keeping the size of N constant while reducing the size of the two distinct prime numbers by calculating N from a product of a first distinct prime number raised to the first power and a second distinct prime number wherein the first power is greater than one and constructing an additional R''_1 using one of the two distinct prime numbers raised to a power greater than one, wherein efficiency of the decryption is increased. However, Takagi teaches that by performing $n = p^k q$, the system is protected from both the number field sieve and elliptic curve methods of attack (§1 & §3 ¶2-3) where p and q are over 256 bits and n is over 768 bits (rather than $n=pq$, where if n is 768 bits, then p and q would be 384 bits). This system is faster than standard RSA (§4, last ¶). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to reduce the size of the two distinct prime numbers while keeping the size of the public key root constant using exponentiation of the two distinct prime numbers and construct an additional R''_1 using one of the two distinct prime numbers raised to a power greater than one/k. One of ordinary skill in the art would have been motivated to perform such a modification to protect the system from attack and to increase speed, as taught by Takagi (§1, §3 ¶2-3 & §4 last ¶).

15. Claims 21-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Menezes in view of Takagi. Menezes discloses standard RSA parameter generation, wherein (n,e) is the public key with n (public key root) =pq (two distinct prime numbers), forming a public RSA key pair/(n, e) by associating the public key root/n and a standard RSA encryption exponent/e (§8.2.1) and computing a private RSA key pair/(n,d) by mathematically combining the standard

RSA encryption exponent/e and the n-bit distinct prime numbers/ $ed \equiv 1 \bmod((p-1)(q-1))$. Menezes lacks reducing the size of the two distinct prime numbers while keeping the size of the public key root constant using exponentiation of the two distinct prime numbers. However, Takagi teaches that by performing $n = p^k q$, (k=2, §4 ¶1) the system is protected from both the number field sieve and elliptic curve methods of attack (§1 & §3 ¶2-3) where p and q are over 256 bits and n is over 768 bits (rather than n=pq, where if n is 768 bits, then p and q would be 384 bits). This system is faster than standard RSA (§4, last ¶). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to reduce the size of the two distinct prime numbers while keeping the size of the public key root constant using exponentiation of the two distinct prime numbers. One of ordinary skill in the art would have been motivated to perform such a modification to protect the system from attack and to increase speed, as taught by Takagi (§1, §3 ¶2-3 & §4 last ¶).

16. Claim 24 is rejected under 35 U.S.C. 103(a) as being unpatentable over Menezes in view of Takagi, as applied to claim 21 above, in further view of Stallings, in further view of U.S. Patent 6,578,061 to Aoki et al. (Aoki). Menezes, as modified above, lacks encrypting a pre-master secret using the public key and decrypting the pre-master secret using the private key and compensating for the reduction in size via Hensle lifting. However, Stallings teaches that encrypting a pre-master secret at a client using an RSA public key (page 217, ¶4) and decrypting the cipher-text at a web server using an RSA private key (page 218, ¶5) is used in SSL. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to encrypt a pre-master secret using the public key and decrypt the pre-master secret using the private key. One of ordinary skill in the art would have been motivated

to perform such a modification to perform SSL, as taught by Stallings (page 217, ¶4 & page 218, ¶5). Further, Aoki teaches that Hensel lifting is a natural method of raising the root of a polynomial from $\bmod b^m$ to $\bmod b^{m+1}$ (col. 5, lines 14-18). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to compensate for the reduction using Hensel lifting. One of ordinary skill in the art would have been motivated to perform such a modification to utilize a natural method of raising the root of a polynomial from $\bmod b^m$ to $\bmod b^{m+1}$, as taught by Aoki (col. 5, lines 14-18).

17. Claim 25 is rejected under 35 U.S.C. 103(a) as being unpatentable over Boneh in view of Stallings in view of Takagi, in further view of Aoki. Boneh discloses all of the elements of the claim (pages 203 and 205), except a web server, keeping the size of N constant while reducing the size of the two distinct prime numbers by calculating N from a product of a first distinct prime number raised to the first power and a second distinct prime number wherein the first power is greater than one and constructing an additional R''_1 using one of the two distinct prime numbers raised to a power greater than one, wherein efficiency of the decryption is increased and using Hensel lifting to compensate for altering the multiplicity of the distinct prime numbers. However, Stallings teaches that the SSL uses RSA encryption to secure communications between a client and a server (page 214). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to include a web server. One of ordinary skill in the art would have been motivated to perform such a modification to secure communications between a server and a client using SSL, as taught by Stallings (page 214). Further, Takagi teaches that by performing $n = p^k q$, the system is protected from both the number field sieve and elliptic curve methods of attack (§1 & §3 ¶2-3) where p and q are over

256 bits and n is over 768 bits (rather than $n=pq$, where if n is 768 bits, then p and q would be 384 bits). This system is faster than standard RSA (§4, last ¶). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to reduce the size of the two distinct prime numbers while keeping the size of the public key root constant using exponentiation of the two distinct prime numbers and construct an additional R''_1 using one of the two distinct prime numbers raised to a power greater than one/k. One of ordinary skill in the art would have been motivated to perform such a modification to protect the system from attack and to increase speed, as taught by Takagi (§1, §3 ¶2-3 & §4 last ¶). Further, Aoki teaches that Hensel lifting is a natural method of raising the root of a polynomial from $\bmod b^m$ to $\bmod b^{m+1}$ (col. 5, lines 14-18). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to compensate for the reduction using Hensel lifting. One of ordinary skill in the art would have been motivated to perform such a modification to utilize a natural method of raising the root of a polynomial from $\bmod b^m$ to $\bmod b^{m+1}$, as taught by Aoki (col. 5, lines 14-18).

18. Claims 26 & 31-32 is rejected under 35 U.S.C. 103(a) as being unpatentable over Boneh in view of Stallings, Takagi and Aoki, in further view of Collins. Claim 26 is substantially equivalent to claim 25 and is rejected under similar rationale, except Boneh, as modified above, further lacks reducing the size of the two distinct prime numbers such that each of the two distinct prime numbers is on the order of one third the size of N. However, Collins teaches that using multi-prime RSA, computational speed is increased (col. 3, lines 35-46). Using, for example 3 primes, each is 100 digits long, rather than a single one at 300 digits long (col. 3, lines 49-55). Therefore, it would have been obvious to one having ordinary skill in the art at the time

the invention was made to reduce the size of the two distinct prime numbers such that each of the two distinct prime numbers is on the order of one third the size of N. One of ordinary skill in the art would have been motivated to perform such a modification to make use of multi-prime RSA to increase computational speed, as taught by Collins (col. 3, lines 35-55).

Conclusion

19. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (703) 305-8191. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m.. The examiner can also be reached on alternate Fridays from 6:45 a.m. – 3:15 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached at (703) 308-4789.

Any response to this action should be mailed to:
Commissioner of Patents and Trademarks
Washington, DC 20231
Or faxed to:
(703)746-7239 (for formal communications intended for entry)
Or:
(703)746-7240 (for informal or draft communications, please label "PROPOSED" or "DRAFT")
Hand-delivered responses should be brought to Crystal Park II, 2121 Crystal Drive, Arlington, VA 22202, Fourth Floor (Receptionist).

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-9000.

NOTE: After October 19, 2004, Michael Simitoski can be reached at (571) 272-3841, Greg Morse can be reached at (571) 272-3838 and general inquiries can be directed to (571) 272-2100.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MJS
September 30, 2004

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100